INFORMATION ASSURANCE

Proponent for Inspection: **Directorate of Information Management** Point of Contact: ______________________________

Unit Inspected: _____________________________ Date of Inspection: ____________________________

Unit Representative: ________________________ Inspector Name: ______________________________

Unit Phone No: __________________________ Inspector's Phone No. __________________________

Unit Overall Rating: T P U

REFERENCES:
a. AR 25-2, Information Assurance, 14 Nov 03
b. DoD 8570.1-M, Information Assurance Workforce Improvement Program, Dec 19, 2005
c. DoDI 8510.bb, Interim DoD Information Assurance Certification and Accreditation Process (DIACAP), Jul 2, 2006
d. AR 25-400-2, ARIMS, 15 Nov 04

STANDARDS:
T= 90% success rate of evaluated tasks with no failed critical tasks.
P= 70% success rate of evaluated tasks with no failed critical tasks.
U= less than 70% success rate of evaluated tasks or one failed critical task.

INSPECTION CRITERIA:	LEVEL	GO	NO GO	REMARKS
1. Does the unit have the most current referenced publications?	BN			
2. Are previous inspection results on file and available for review? (IAW AR 25-400-2, Para 6-1)	BN			
3. Does all Army Information Systems (AIS) have approved and licensed software running on them? (IAW AR 25-2 Para 4-6 g. and k.)	BN			
4. **CRITICAL:** Are Information Assurance Security Officers (IASO), Primary/Alternate and System Administrator (SA) appointed? (IAW AR 25-2, Para 3-2 and 3-3)	BN			
5. **CRITICAL** Have System Administrators signed the IS Privileged Access Agreement and Acknowledgment of Responsibilities. (IAW DoD 8570.1-M, Para C3.2.4.4)	BN			
6. **CRITICAL:** Are appointed IA Security personnel properly trained and certified? (IAW AR 25-2, Para 4-3) (DoD8570.1-M, Para C 2.3)	BN			
7. **CRITICAL:** Have all IA Security personnel input their IA training in the Asset & Vulnerability Tracking Resource (A&VTR)? (IAW AR 25-2 Para 4-5, r3)	BN			
8. **CRITICAL:** Are security incidents reported to the Information Assurance Manager & RCERT as required? (IAW AR 25-2 Para 4-22)	BN			
9. **CRITICAL:** Have all AIS users in the Command reviewed and acknowledged the FLW Acceptable Users Policy (AUP)? (IAW 25-2, Para 4-5 r3)	BN			
10. **CRITICAL:** Have all network accounts inactive for more than 45 days disabled or deleted? (IAW AR 25-2 Para 3-3 a.(10)?	BN			
11. **CRITICAL:** Is there a Risk Analysis/Vulnerability Assessment in place? (IAW AR 25-2, Para 7-1)	BN			
12. **CRITICAL:** Are all users receiving initial and Annual Information Assurance training and awareness briefings that include threat identification, physical security, acceptable use policy, malicious content and other non-standard threats? (IAW AR 25-2, Para 3-3 c.(1)(b)	BN			
13. **CRITICAL:** Does all AIS have the current and supportable version of AntiVirus software configured to provide real-time protection? (IAW AR 25-2, Para. 4-5 n.(2)(a)	BN			
14. **CRITICAL** Have all Information Systems within the organization been accredited? (IAW AR 25-2 Para 4-5 a and DoDI 8510.bb)	BN			
15. **CRITICAL:** Has the IAM been provided a copy of current Approval To Operate (ATO) or Interim Approval To Operate (IATO) and complete C&A documentation for unique systems under the control of the inspected unit? (IAW AR 25-2, Para 5-6 a.)	BN			
REMARKS:				